EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# ENISA TRANSPORT THREAT LANDSCAPE

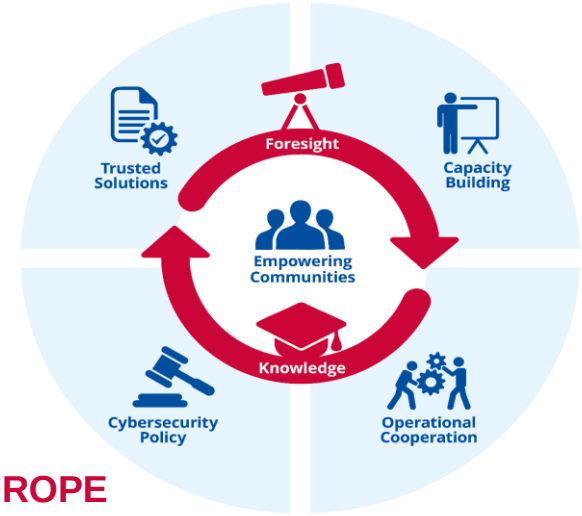
Ricardo Figueiredo
Policy Development and Implementation Unit

14 | 10 | 2022

# ROLE OF ENISA – WHO WE ARE

Established in 2004, ENISA currently operates under Regulation 2019/881, often referred to as the 'Cybersecurity Act'

- Development and implementation of EU policy and law, including by supporting the EU Member States
- Assistance with capacity-building, for example in developing national CSIRTs
- Supporting operational cooperation at EU level
- Development of EU cybersecurity certification framework
- Increasing the level of cybersecurity knowledge and information
- Raising cybersecurity awareness
- Contributing to research and innovation
- Fostering international cooperation




**A TRUSTED AND CYBER SECURE EUROPE**

# ENISA THREAT LANDSCAPE TRADITION


**It's reflecting on the PAST to prepare for the FUTURE**

10 YEARS

# THE TRANSPORT THREAT LANDSCAPE

- Main driver: Impactful threats observed in the sector, suggesting an analysis per se
- Objectives: identify threats, threat actors, TTPs, etc | observe notable trends | identify opportunities for increasing the resilience on the sector
- Scope: Strategic, structuring information for sharing and decision making
- Sectors: Maritime, Air, Rail, Road
- Data: Mostly open source and reported incidents
- Processing : ENISA taxonomy and MITRE framework
- Reporting period: January 2021-June 2022

# MARITIME SECTOR – PRIME THREATS

Preliminary Findings

1. Ransomware attacks (and malware)

2. Data leakage, exfiltration, and data breach

- Phishing or brute force attacks as the entry point

- Main targets are:
  - IT (business side of the system)
  - Maritime services (vessel berthing services, vessel loading/unloading services, temporary storage & staying services, website, display boards, servers, passengers' personal data, support services, security, and safety services etc.)

# MARITIME SECTOR – REPORTED INCIDENTS' SAMPLE

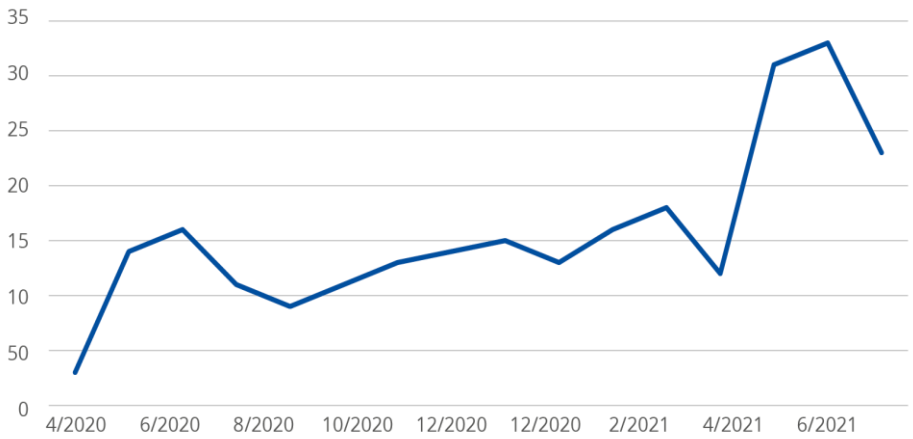
Non Exhaustive

| Country | Short Description | Type | Actor |
|---|---|---|---|
| BE | Ghent port giant Sea-Invest fell by cyber attack | Ransomware | Cyber-criminal |
| IN | Ransomware attack hits Nhava Sheva container terminal | Ransomware | Malicious Insider |
| FR | Boat Building Giant Beneteau Says Cyberattack Disrupted Production | Ransomware | Cyber-criminal |
| US | Steamship Authority hit by ransomware attack | Ransomware | Cyber-criminal |
| FR<br>UK<br>GLOBAL | Secret files show alleged Iranian plans to sink ships using cyberattacks | Hybrid | N/A |
| CH | CGN victim of a cyberattack on its website | Exfiltration<br>Data leakage<br>Breach | Cyber-criminal |
| FR | CMA CGM confirms data leak after cyber attack | Exfiltration<br>Data Leakage<br>Breach | Cyber-criminal |
| GLOBAL<br>IS | Microsoft Says 'Iran-Linked' Hackers Targeted US, EU, Israeli Defense & Maritime Sectors | Credential stuffing attack | N/A |
| GR | DANAOS shipping company cyber-attacked | N/A | Cyber-criminal |
| UK | Maritime giant Swire Pacific Offshore suffers data breach following cyber-attack | Ransomware | Cyber-criminal |

# FINDINGS FROM ETL FOR RANSOMWARE ATTACKS


## Ransomware was the prime threat for 2021

*"The average ransom doubled in 2020. Highest paid ransom passed $10 million ($11 Million, JBS, Revil, June 2021)"*




*"Conti and ransomware groups lead the 'market'"*

*"Increased usage of zero-day vulnerabilities"*

*"A shift from double to triple extortion"*

***RDP and phishing remain the most common attack vectors***

*"Ransomware-as-a-Service business model"*

*"The volatility of ransomware groups; shutdowns and arrests"*

# FINDINGS FROM ETL FOR RANSOMWARE ATTACKS

**Lack of reliable data…**

Total number of ransomware reported incidents from May 2021 to June 2022 was **3,640**

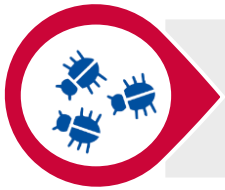
**Initial access in only known for only 29 incidents**

**Either they don't know or have not shared…**

**Ransom unfortunately is being paid**

**(around 60% probably have paid)**

# FINDINGS FROM ETL FOR RANSOMWARE ATTACKS



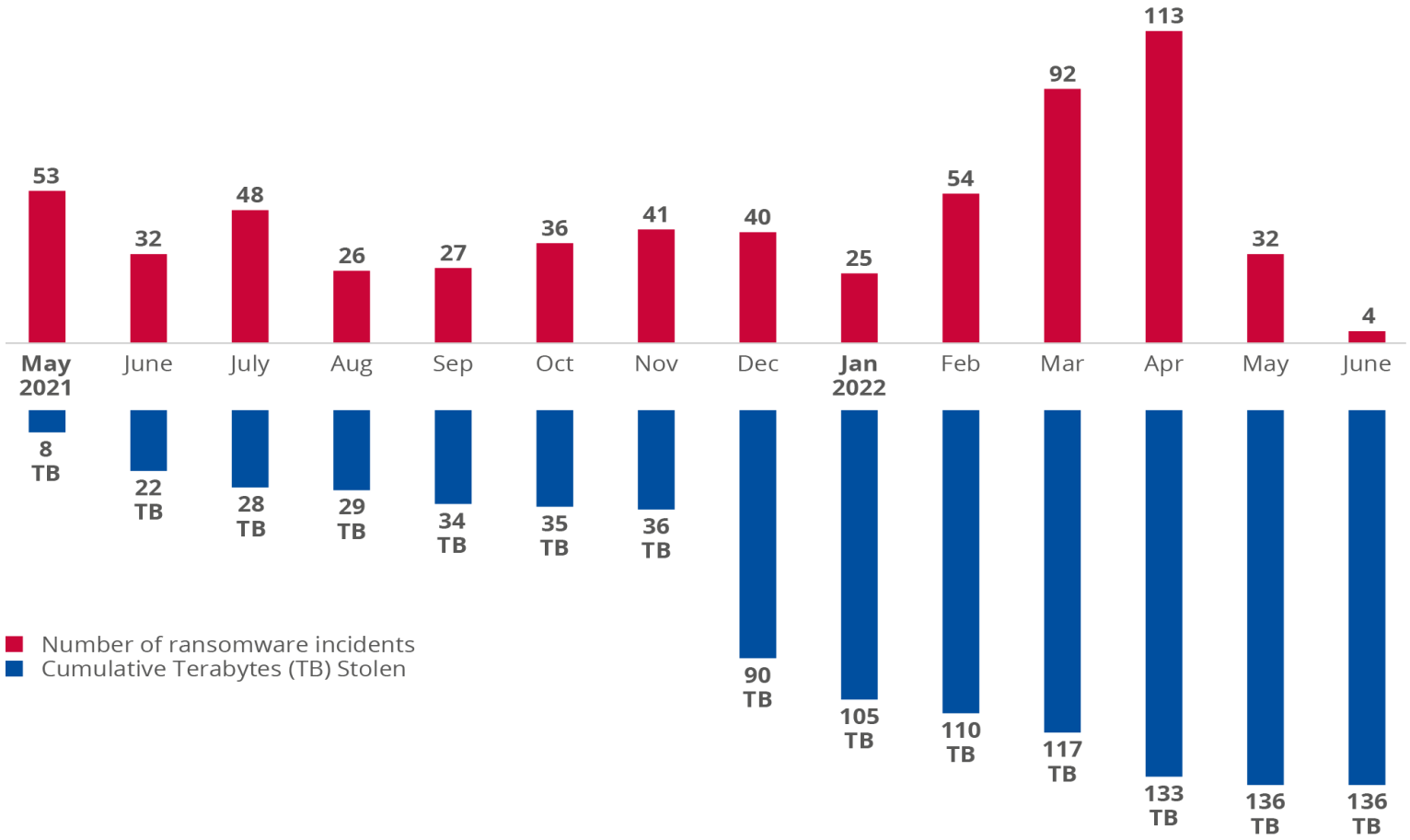
They don’t really seem to care about the sector

**47 different groups**

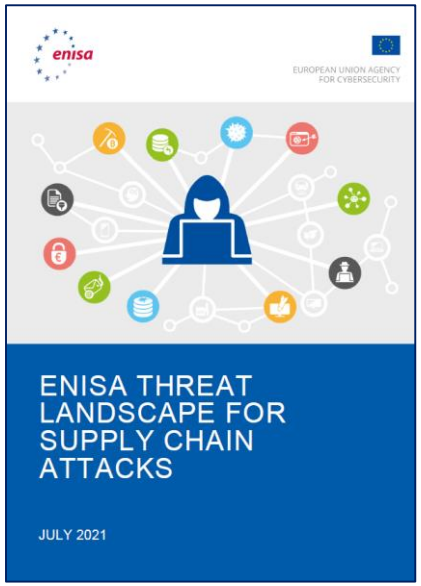
**RaaS makes it hard to identify the threat actor behind an attack**

**10 TB per month** leaked..

# STOLEN DATA VS RAMSOMWARE INCIDENTS

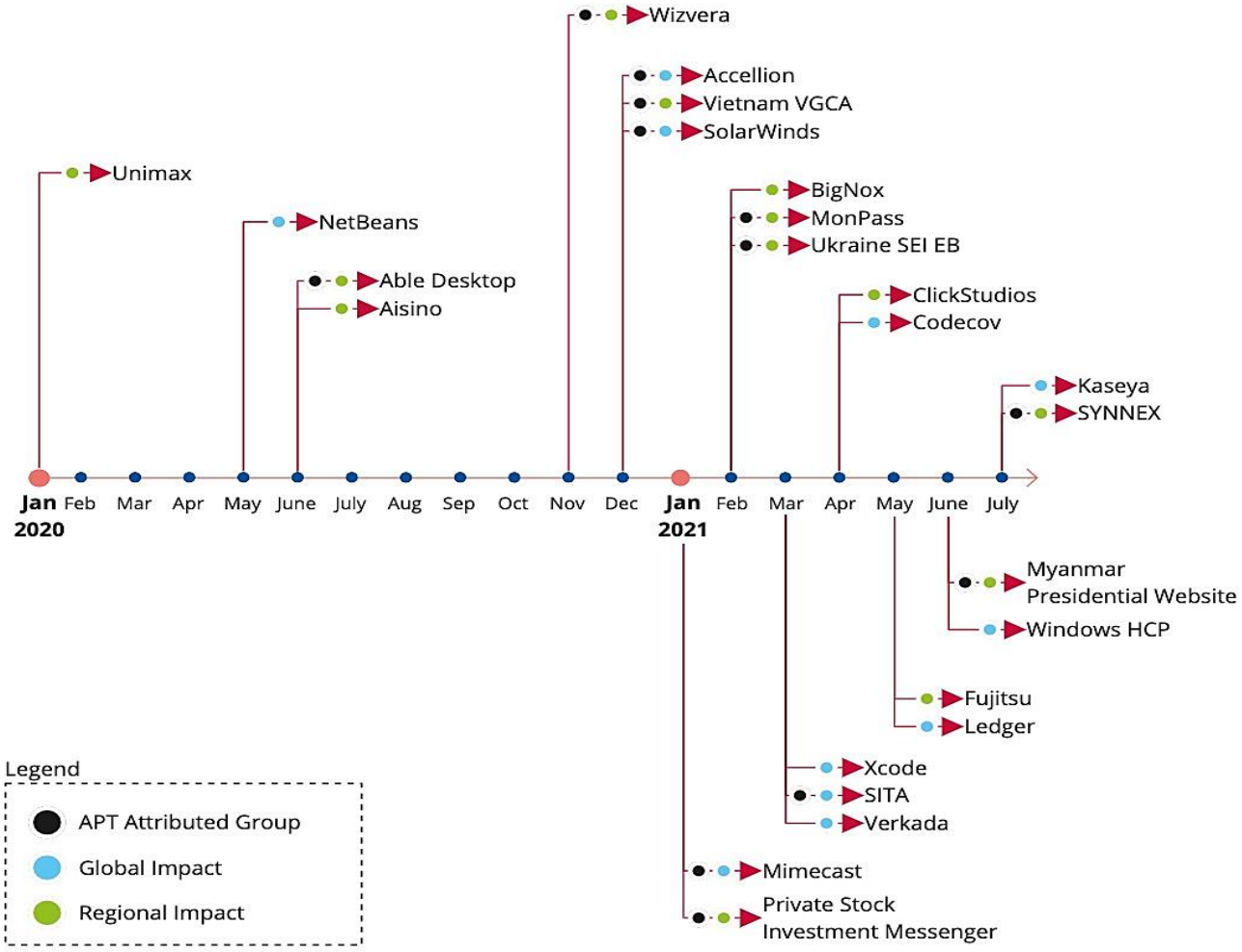


# FINDINGS FROM ETL FOR SUPPLY CHAIN ATTACKS (2021)




- More than 50% conducted by state sponsored attackers and well-known cybercrime groups.
- Around 62% of the attacks on customers took advantage of their trust in their supplier.
- In 66% of the incidents, attackers focused on the suppliers' code in order to further compromise targeted customers.
- Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property).

# TIMELINE OF SUPPLY CHAIN ATTACKS




Available data (2020-2021) suggests that supply chain attacks will most likely increase, moving forward.

# STAY TUNED - HTTPS://WWW.ENISA.EUROPA.EU/

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, pu

TOPICS | PUBLICATIONS | TOOLS | NEWS | EVENTS

## ENISA Threat Landscape 2021

This is the ninth edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape that identifies prime threats, major trends observed with respect to threats, threat actors and attack techniques, and also describes relevant mitigation measures. In the process of constantly improving our methodology for the development of threat landscapes, this year's work has been supported by a newly formatted ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL). In this report we discuss the first 8 cybersecurity threat categories. Supply chain threats, the 9th category, were analysed in detail, in a dedicated ENISA report.

**Published** October 27, 2021
**Language**


Download
PDF document, 5.25 MB

# THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 152 31
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu